DISK DRIVE EMPLOYING A DISK WITH A PRISTINE AREA FOR STORING ENCRYPTED DATA ACCESSIBLE ONLY BY TRUSTED DEVICES OR CLIENTS TO FACILITATE SECURE NETWORK COMMUNICATIONS

CROSS-REFERENCE TO RELATED PATENTS AND APPLICATIONS

This patent application is related to other co-pending U.S. patent applications. Namely, U.S. patent application serial no. 09/608,103 entitled "SECURE DISK DRIVE COMPRISING A SECURE DRIVE KEY AND A DRIVE ID FOR IMPLEMENTING SECURE COMMUNICATION OVER A PUBLIC NETWORK," and serial no. 09/608,102 entitled "DISK DRIVE IMPLEMENTING KEY MANAGEMENT FOR GENERATING AND DECOMMISSIONING CLIENT KEYS SUPPLIED TO CLIENT COMPUTERS TO FACILITATE SECURE COMMUNICATION OVER A PUBLIC NETWORK."

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to disk drives for computer systems. More particularly, the present invention relates to a disk drive employing a disk with a pristine area for storing encrypted data accessible only by trusted devices or clients to facilitate secure network communications.

Description of the Prior Art

Cryptography for secure network communications is typically implemented by server and client computers attached to a network. With Internet communications, for example, cryptography is typically implemented by the server computers hosting secure web sites and the browser programs running on client computers. A secure communication protocol, such as the Secure Socket Layer (SSL), is used to transmit encrypted messages over public lines subject to inspection. If an encrypted message is intercepted while in transit, it is extremely difficult to

decipher the message without the cryptographic key. For this reason, attackers are focusing their efforts on the computers which implement the cryptography algorithms in an attempt to glean information about the secret cryptographic keys used for the authentication and the encryption/decryption operations. The attacks may be physical using debuggers and logic analyzers, or they may be remote attacks using virus programs which invade the computer's operating system in order to obtain information concerning the cryptographic keys. A virus may, for example, be introduced remotely into a computer's operating system by attaching the virus to an email.

A paper by H. Gobioff, G. Gibson, and D. Tygar entitled "Security for Network Attached Storage Devices", October 23 1997, School of Computer Science, Carnegie Mellon University, suggests to implement cryptography algorithms and secret keys in tamper resistant circuitry within a disk drive where it is less susceptible to probing and virus attacks. These types of disk drives, referred to as NASD disk drives, are intended to be attached directly to a network in order to avoid the overhead associated with an intervening file server. However, the above referenced paper does not disclose many details of implementation, particularly with respect to the authentication and encryption/decryption operations.

The Digital Transmission Content Specification or DTCP (available through the Internet at http://www.dtcp.com) discloses a cryptographic protocol for protecting audio/video (A/V) content from unauthorized copying as it traverses digital transmission mechanisms from device to device. Only compliant devices manufactured to support the DTCP protocol are capable of transmitting or receiving the protected A/V content. Each device is manufactured with a unique device ID and a public/private key pair which facilitate authentication and encryption/decryption of the A/V content. The DTCP specification suggests to store the private key in a way so as to prevent its disclosure, however, no specific means are disclosed for achieving this objective.

U.S. Patent No. 5,931,947 discloses a network storage device for use in a secure array of such devices to support a distributed file system. Each device is an independent repository of remotely encrypted data to be accessed by authorized network clients. All encryption is done by

the clients, rather than by the devices, and the encrypted data is stored in encrypted form. Each network storage device comprises an owner key used to generate authentication keys within the device for authenticating messages received from the clients. However, the keys used by the clients for encrypting data and generating the message authentication codes are generated external to the devices by a system administrator which is susceptible to attack. Further, the aforementioned patent does not disclose any details concerning the privacy of the owner key within each disk drive.

U.S. Patent No. 5,687,237 discloses an encryption key management system for an integrated circuit which encrypts or decrypts data received from a microcontroller. The encryption and decryption operations are implemented using cryptographic keys stored in a non-volatile memory in encrypted form to protect against discovery. When needed to encrypt or decrypt data, the integrated circuit employs a secret internal key to decrypt the cryptographic keys stored in the non-volatile memory. Although storing the cryptographic keys in encrypted form protects against discovery, the aforementioned patent does not disclose any details concerning the authentication of users or devices requesting the encryption or decryption operations, nor does it disclose any details concerning the authentication of messages to verify that the messages have not been modified while in transit over public lines.

There is, therefore, the need to improve security in network communications, particularly with respect to probing attacks and virus attacks on computer operating systems.

SUMMARY OF THE INVENTION

The present invention may be regarded as a disk drive comprising a disk for storing data, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data. The disk drive comprises a head for reading the encrypted data from the pristine area of the disk, and a control system for controlling access to the pristine area of the disk. Authentication circuitry within the disk drive is provided for authenticating a request received from an external entity to access the pristine area of the disk and for enabling the control system if the request is authenticated. The disk drive further comprises a secret drive key, and

decryption circuitry responsive to the secret drive key, for decrypting the encrypted data stored in the pristine area of the disk.

The present invention may also be regarded as a disk drive comprising a disk for storing data, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data. The disk drive comprises a head for reading data from the disk, and a control system for controlling access to the disk. The disk drive further comprises a secret drive key, and decryption circuitry responsive to the secret drive key, for decrypting the encrypted data stored in the pristine area of the disk to generate decrypted data. The decrypted data is processed by authentication circuitry within the disk drive for authenticating a request received from an external entity to access the disk and for enabling the control system if the request is authenticated.

The present invention may also be regarded as a disk drive comprising a disk for storing data, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data. The disk drive comprises a head for reading the encrypted data from the pristine area of the disk, and a control system for controlling access to the pristine area of the disk. The disk drive further comprises a secret drive key, and decryption circuitry responsive to the secret drive key, for decrypting the encrypted data stored in the pristine area of the disk. The disk comprises a plurality of physical blocks accessed by the control system through physical block addresses. An access request received from an external entity during normal operation of the disk drive comprises a logical block address which is mapped by the control system to a selected one of the physical block addresses. The pristine area comprises at least one physical block written with at least part of the encrypted data during manufacturing of the disk drive and not externally accessible through a logical block address during normal operation of the disk drive.

The present invention may also be regarded as a method of processing a request received by a disk drive from an external entity to access encrypted data stored in a pristine area of a disk. The method comprises the steps of authenticating the request to access the pristine area and enabling access to the pristine area if the request is authenticated, reading the encrypted data

stored in the pristine area, and decrypting the encrypted data using a secret drive key within the disk drive to generate decrypted data.

The present invention may also be regarded as a method of processing a request received by a disk drive from an external entity to access data stored on a disk, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data. The method comprises the steps of decrypting the encrypted data stored in the pristine area of the disk using a secret drive key within the disk drive to generate decrypted data, and using the decrypted data to authenticate the request received from the external entity before allowing access to the disk.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a disk drive according to an embodiment of the present invention comprising a disk having a public area for storing plaintext data and a pristine area for storing encrypted data, decryption circuitry for decrypting the encrypted data, a secret drive key employed by the decryption circuitry, and authentication circuitry for authenticating requests by external entities to access the pristine area.

FIG. 2 shows a disk drive according to an embodiment of the present invention wherein the authentication circuitry is responsive to decrypted data generated by the decryption circuitry after decrypting the encrypted data stored in the pristine area of the disk.

FIG. 3 shows an embodiment of the present invention wherein the authentication circuitry implements a challenge and response protocol in order to verify the authentication of a user or a device, wherein the pristine area on the disk is used to store data employed in the challenge and response protocol.

FIG. 4 shows a disk format according to an embodiment of the present invention as comprising a plurality of physical blocks in the pristine area which are written with encrypted data during manufacturing and are not externally accessible during normal operation of the disk drive.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. 1 shows a disk drive 2 according to an embodiment of the present invention

comprising a disk 4 for storing data, the disk 4 comprising a public area 6 for storing plaintext data and a pristine area 8 for storing encrypted data. The disk drive 2 comprises a head 10 for reading the encrypted data from the pristine area 8 of the disk 4, and a control system 12 for controlling access to the pristine area 8 of the disk 4. Authentication circuitry 14 within the disk drive 2 is provided for authenticating a request received from an external entity to access the pristine area 8 of the disk 4 and for enabling the control system 12 if the request is authenticated. The disk drive 2 further comprises a secret drive key 16, and decryption circuitry 18 responsive to the secret drive key 16, for decrypting the encrypted data stored in the pristine area 8 of the disk 4.

In the embodiment of FIG. 1, the disk drive further comprises a preamplifier 20 for generating an analog write signal 22 supplied to the head 10 during a write operation and for receiving an analog read signal 22 from the head 10 during a read operation. The preamplifier 20 receives digital write data 24 from the control system 12 which is to be written to the disk 4, wherein the digital write data 24 modulates current in the analog write signal 22 and thus the head 10 in order to write a series of magnetic transitions on the surface of the disk 4 representing the recorded digital data. During a read operation, the head 10 senses the magnetic transitions which induces pulses in the analog read signal 22. The preamplifier 20 preamplifies the analog read signal 22 and the preamplified analog read signal 26 is supplied to the control system 12 where it is demodulated into an estimated data sequence representing the originally recorded data. In one embodiment, the control system 12 implements an error correction code (ECC) for use in detecting and correcting errors in the estimated digital data induced by the recording and reproduction process. The control system 12 sends control sequences to the preamplifier 20 over line 28 in order to configure it for write or read operations.

In the embodiment of FIG. 1, the head 10 is mounted on the distal end of an actuator arm 32 which is rotated about a pivot 34 by a voice coil motor (VCM not shown). The control system 12 comprises a servo control system for generating control signals 36 applied to the VCM in order to position the head radially over the disk 4 so as to access a desired area of the disk 4

during write and read operations. The control system 12 will access the pristine area 8 and allow a write or read operation only if certain predetermined conditions are satisfied.

In one embodiment of the present invention, the disk drive 2 receives requests from external entities (e.g., a host or client computer) to access the pristine area 8. The control system 12 allows the access only if the request is authenticated by the authentication circuitry 14. For example, the pristine area 8 may store sensitive information (e.g., a password, credit card number, etc.) for use in a secure transaction with an Internet web site. This information is stored in the pristine area 8 in encrypted form so that it cannot be discovered by an attacker evaluating the disk storage medium. In addition, the pristine area 8 is protected from access through normal operation of the disk drive 2 by requiring requests received from external entities to be authenticated.

When the control system 12 receives via line 38 a request from an external entity to access the pristine area 8 (read or write), it sends a command via line 40 to the authentication circuitry 14 to authenticate the request. The authentication circuitry 14 evaluates the request and, if authentic, sends a command via line 42 to enable the control system 12 to perform the request. In one embodiment of the present invention, the authentication circuitry 14 enables the servo control system within control system 12 to restrict access to the pristine area 8. Embedded servo sectors are recorded on the disk 4, wherein the embedded servo sectors comprise servo bursts used for servoing the head over the disk 4. In one embodiment, the servo sectors are recorded in unencrypted form in the pristine area 8 such that servoing the head 10 by reading the servo bursts is possible if the disk 4 is removed and placed in another disk drive or on a spin stand. In another embodiment, the servo bursts are recorded in the servo sectors of the pristine area 8 in encrypted form to protect against an attacker removing the disk 4 and attempting to servo using an external apparatus. In one embodiment, the servo bursts are encrypted by recording the servo bursts with additive noise generated from a pseudo random sequence. The pseudo random sequence is generated using a polynomial, and the authentication circuitry provides the polynomial to the control system 12 to enable the servo control system to servo in the pristine

area 8. The additive noise in the servo bursts is subtracted from the read signal by regenerating the pseudo random sequence. In one embodiment, the polynomial for regenerating the pseudo random sequence is stored in encrypted form in the pristine area 8 of the disk 4, preferably in a physical block which is inaccessible to an external entity as described in greater detail below with reference to FIG. 4.

In another embodiment of the present invention shown in FIG. 2, the authentication process is implemented using the encrypted data stored in the pristine area 8. The encrypted data is read from the disk 4 by the control system 12, decrypted by the decryption circuitry 18 using the secret drive key 16, and the decrypted data transferred over line 44 to the authentication circuitry 14.

The authentication circuitry 14 may perform user/device authentication, message authentication, or user/device as well as message authentication. With user/device authentication, the authentication circuitry 14 verifies that the request was sent from a trusted entity, and with message authentication, the authentication circuitry 14 verifies that the request was not modified while in transit from the external entity to the disk drive 2.

User/device authentication may be implemented, for example, by associating selected information (e.g., a password, finger print, voice print, spectral signature, etc.) with a trusted entity. In one embodiment, user/device authentication information (e.g., a password) is stored in the pristine area 8 of the disk 4. When an external entity sends a request to access to the pristine area 8, the request received over line 38 comprises an entity ID and an entity password. The authentication circuitry 14 uses the entity ID to read the associated password from the pristine area 8, and the request is authenticated if it matches the entity password received in the request. Otherwise, the request is not authenticated and access is denied.

The user/device authentication information (e.g., password) is stored in the pristine area 8 in encrypted form using a suitable encryption algorithm (e.g., DES, RSA, etc.) which may be symmetric (private key encryption) or asymmetric (public key encryption). The decryption circuitry 18 within the disk drive 2 uses the secret drive key 16 to decrypt the encrypted

authentication information, and the decrypted authentication information is provided to the authentication circuitry 14 over line 44 (FIG. 2). A suitable means is employed to protect the secret drive key 16 from discovery, such as tamper resistant circuitry. In addition, all or part of the control system 12 and/or the authentication circuitry 14 may be implemented using tamper resistant circuitry to protect the decrypted authentication data. An example discussion of tamper-resistant circuitry is provided in Tygar, J.D. and Yee, B.S., "Secure Coprocessors in Electronic Commerce Applications," Proceedings 1995 USENIX Electronic Commerce Workshop, 1995, New York, which is incorporated herein by reference.

In the above referenced co-pending patent application entitled "SECURE DISK DRIVE COMPRISING A SECURE DRIVE KEY AND A DRIVE ID FOR IMPLEMENTING SECURE COMMUNICATION OVER A PUBLIC NETWORK," a nexus of secure disk drives are manufactured in a way that enables secure network communication between the drives. In one embodiment, each secure disk drive is manufactured with a secure drive key and a unique drive ID which are used for identification and authentication. When the network detects that one of the secure disk drives has been compromised, its drive ID is invalidated. Each secure disk drive in the nexus stores a list of invalidated drive IDs. If a secure disk drive receives a request from a disk drive with an invalid drive ID, the request is denied.

In one embodiment of the present invention, the list of invalidated drive IDs is stored in encrypted form in the pristine area 8 of the disk 4 within each secure disk drive. When a request is received over line 38 from a secure disk drive in the nexus, the list of invalidated drive IDs is read from the pristine area 8, decrypted by the decryption circuitry 18 using the secret drive key 16, and transmitted over line 44 (FIG. 2) to the authentication circuitry 14. The authentication circuitry 14 authenticates the secure disk drive (device) by comparing the drive ID received in the request to the list of invalidated drive IDs. In one embodiment, the list of invalidated drive IDs is encrypted according to a message authentication code to protect against attempts to modify the list, wherein the list itself is stored in unencrypted form. Thus, the term "encrypted data" as used herein includes encryption using a message authentication code.

The drive ID in each secure disk drive may also be stored in the pristine area 8 in encrypted form. When a secure disk drive generates a request, the drive ID is read from the pristine area 8, decrypted by the decryption circuitry 18 using the secret drive key 16, and appended to the request.

In an alternative embodiment of the present invention shown in FIG. 3, the pristine area 8 stores information used to implement a suitable challenge and response sequence. A challenge and response sequence is used to authenticate an external entity by sending a random challenge value to the external entity; the external entity is authenticated if it replies with the appropriate response value. In one embodiment, the pristine area 8 stores information used to generate the random challenge value sent to an external entity as well as information for verifying the response value received from the external entity. In another embodiment, the pristine area 8 stores information used to generate the response value for replying to a challenge received from an external entity. The challenge and response information is stored in encrypted form in the pristine area 8, decrypted by the decryption circuitry 18 using the secret drive key 16, and the decrypted data transferred to the authentication circuitry 14 over line 44.

The authentication circuitry 14 may also be used to authenticate a request (message) received from an external client to verify that the request was not modified while in transit. In one embodiment, a message authentication code (MAC) is generated and appended to the request. The request is then authenticated by regenerating the MAC and comparing the regenerated MAC to the MAC appended to the request. If the request has not been modified while in transit, the regenerated MAC will match the MAC appended to the request. Any suitable method may be employed to generate the MAC, for example, using a hashing function implemented with or without a secret key. The pristine area 8 is used to store information in encrypted form for use in generating the MAC, such as a hashing function and/or a secret key used with the hashing function. The MAC information is read from the pristine area 8, decrypted by the decryption circuitry 18 using the secret drive key 16, and transferred to the authentication circuitry 14 over line 44 (FIG. 2).

In another embodiment of the present invention, the pristine area 8 of the disk 4 stores an encrypted secret key for use in decrypting a message received over line 38 from an external entity. The encrypted secret key is read from the pristine area 8 and decrypted by the decryption circuitry 18 using the secret drive key 16. The decrypted secret key is then used by the decryption circuitry 18 to decrypt the message received over line 38. This embodiment may facilitate a distributed key management system for a network of computer devices.

In yet another embodiment of the present invention, the pristine area 8 of the disk 4 stores encrypted message data. An external entity (e.g., a host, client or server) may send a request to the disk drive 2 to store sensitive information (e.g., a credit card number) in the pristine area 8 in encrypted form. The information may already be encrypted before receipt by the disk drive 2, or it may be encrypted by the disk drive 2 before it is written to the pristine area 8. A subsequent request may then be sent to the disk drive 2 to read the encrypted message stored in the pristine area 8. The disk drive 2 will authenticate the request before allowing access to the pristine area 8, and optionally decrypt the message before transferring it to the external entity.

In another embodiment of the present invention, the disk drive 2 of FIG. 1 authenticates a request received from an external entity to access the public area 6 of the disk 4 (read or write). This embodiment provides additional protection in that all requests to access the disk 4, including requests to access the public area 6, must first be authenticated. As with the previously disclosed embodiments, this embodiment implements user/device authentication, and optionally message authentication, using encrypted authentication data stored in the pristine area 8 of the disk 4.

FIG. 4 illustrates another embodiment of the present invention wherein the disk 4 comprises a plurality of physical blocks accessed by the control system using physical block addresses. An access request received from an external entity during normal operation of the disk drive 2 comprises a logical block address which is mapped by the control system 12 to a selected one of the physical block addresses. The pristine area 8 comprises at least one physical block written with at least part of the encrypted data during manufacturing of the disk drive 2 and

not externally accessible through a logical block address during normal operation of the disk drive 2.

Each entry in the table of FIG. 4 represents a physical block recorded on the disk 4, where the first 40 entries (0-39) are the physical blocks reserved for the pristine area 8 and the next 110 entries (40-149) are the physical blocks reserved for the public area 6. The first 20 physical bocks in the pristine area 8 are reserved for storing encrypted data which is inaccessible by external entities through a logical block address during normal operation of the disk drive 2. These physical blocks store encrypted data used internally by the disk drive 2, for example, encrypted authentication information for implementing a challenge and response verification sequence. The encrypted data is written to these physical blocks during manufacture of the disk drive 2 and accessed by the control system 12 using physical block addresses which are not mapped from logical block addresses. The next 20 physical blocks (20-39) in the pristine area 8 are reserved for storing encrypted data which is accessible only by trusted external entities through logical block addresses, that is, after having been authenticated by the authentication circuitry 14.

Partitioning the disk 4 into a public area 6 and a pristine area 8 improves the disk drive's performance. The disk drive's latency and throughput degenerate when accessing the pristine area 8 due to the overhead associated with the decryption circuitry 18 decrypting the encrypted data as it is read from the pristine area 8. However, there are typically fewer accesses to the pristine area 8 as compared to the public area 6. For example, authenticating a request received from an external entity may require only a few accesses to the pristine area 8, whereas the request itself may require multiple accesses (read or write) to the public area 6.

The pristine area 8 may be used to store plaintext data as well as encrypted data, and the public area 6 may be used to store encrypted data as well as plaintext data. For example, it may be desirable to store plaintext data in the pristine area 8 in order to restrict access to the data without degrading the performance of the disk drive. In another embodiment, it may be desirable to store encrypted data in the public area 6 when restricting access to the encrypted data is not a

concern.

In another embodiment of the present invention, a plurality of computer devices, including a plurality of disk drives, are interconnected in a computer network and communicate through a network protocol. Each disk drive comprises a disk having a public area 6 for storing plaintext data and a pristine area 8 for storing encrypted data. Further, each disk drive implements one or more of the aspects described above with respect to restricting access to the pristine area 8, storing encrypted authentication data in the pristine area 8, or partitioning the pristine area 8 into a number of physical blocks accessible by external entities and a number of physical blocks inaccessible by external entities.